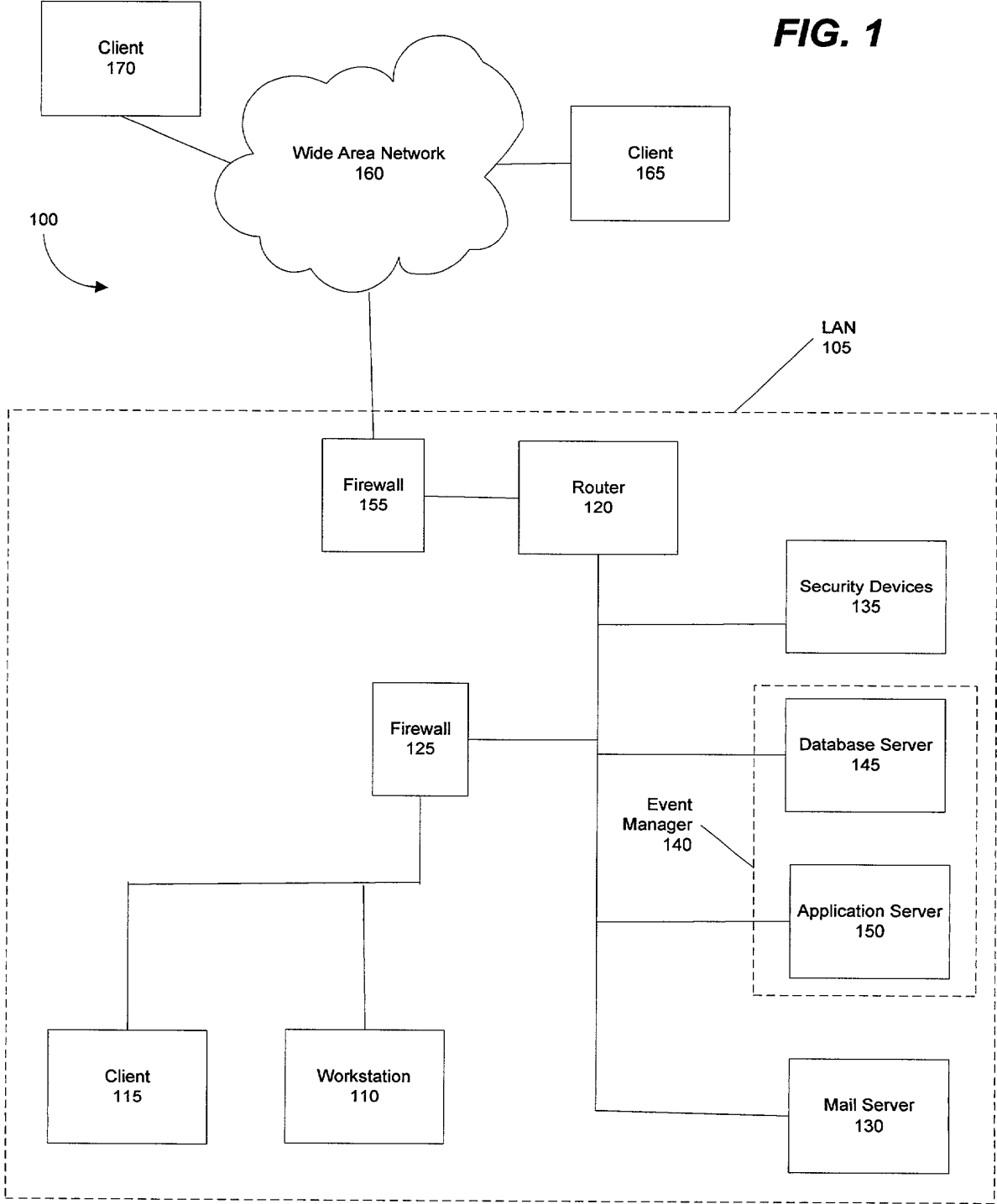


NETWORK
ENVIRONMENT

FIG. 1



ARCHITECTURE

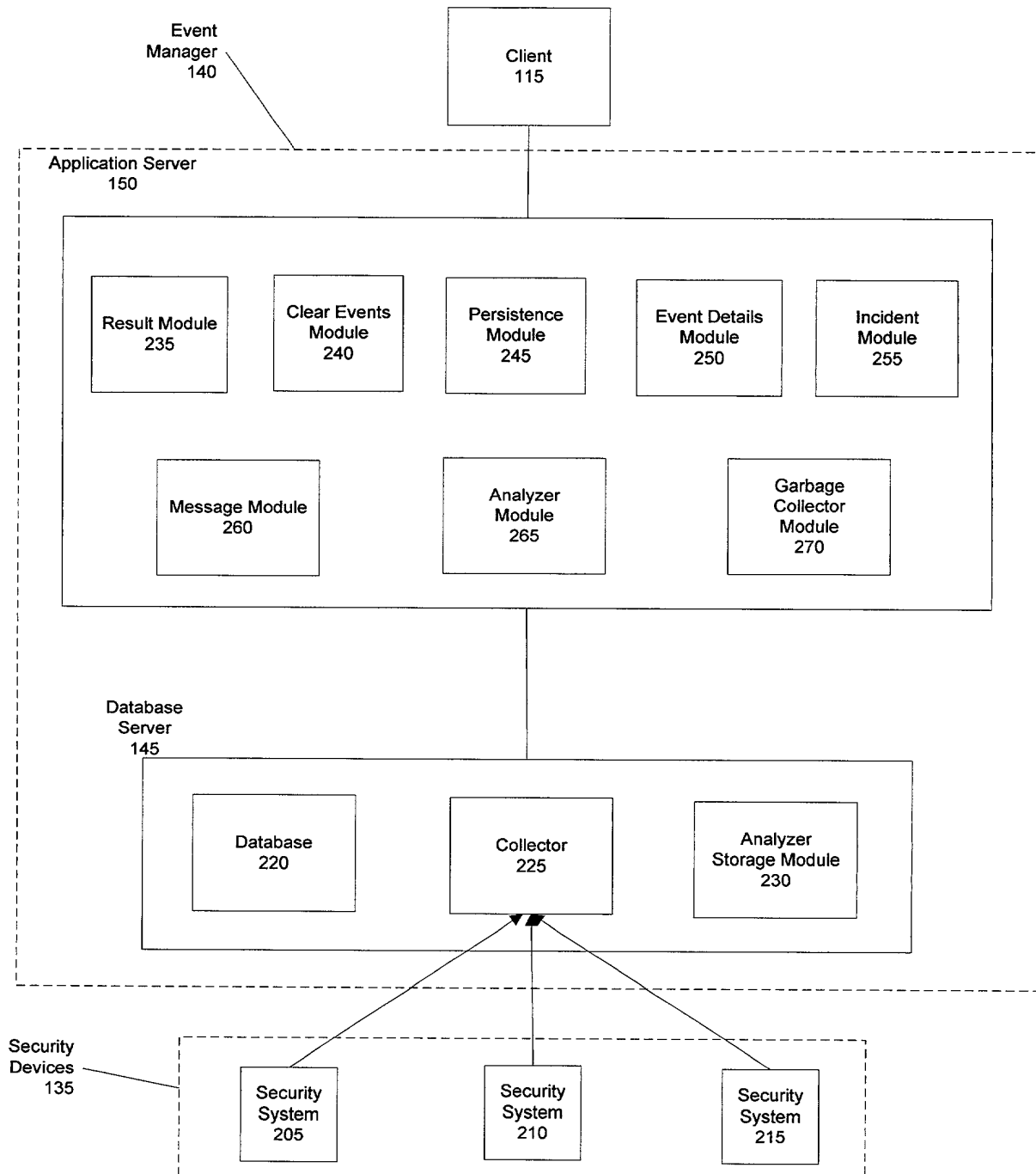


FIG. 2

OVERVIEW

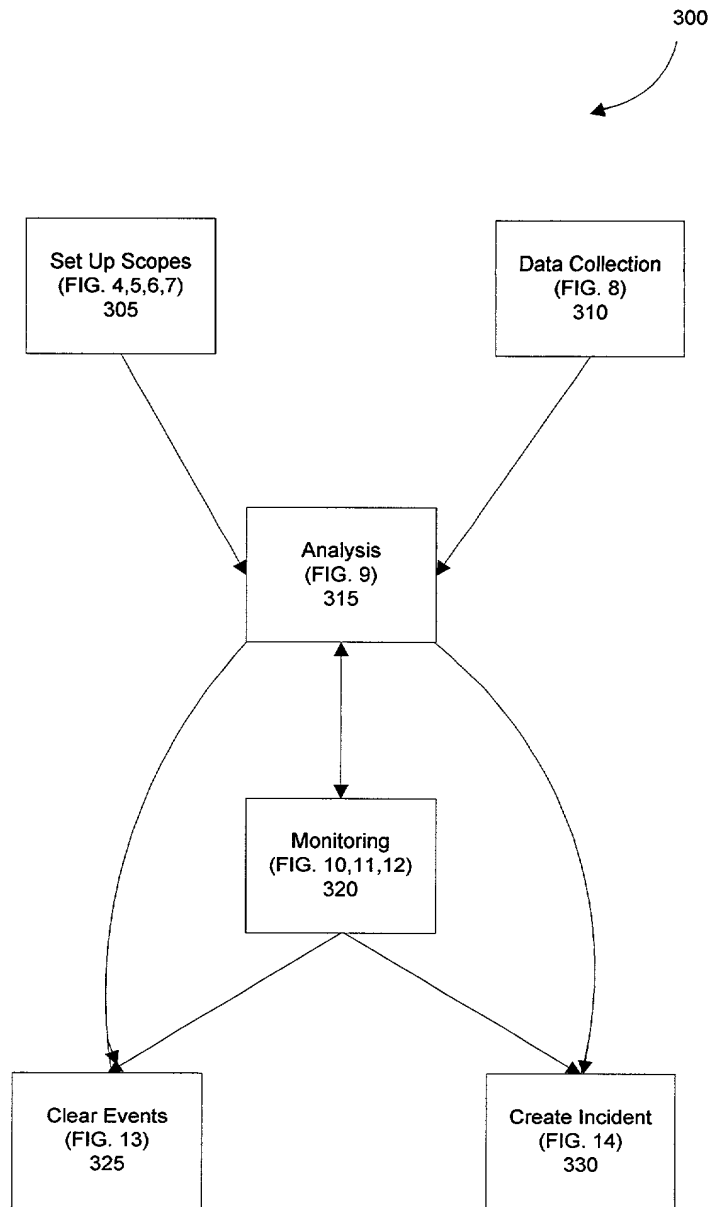


FIG. 3

OPEN A SCOPE

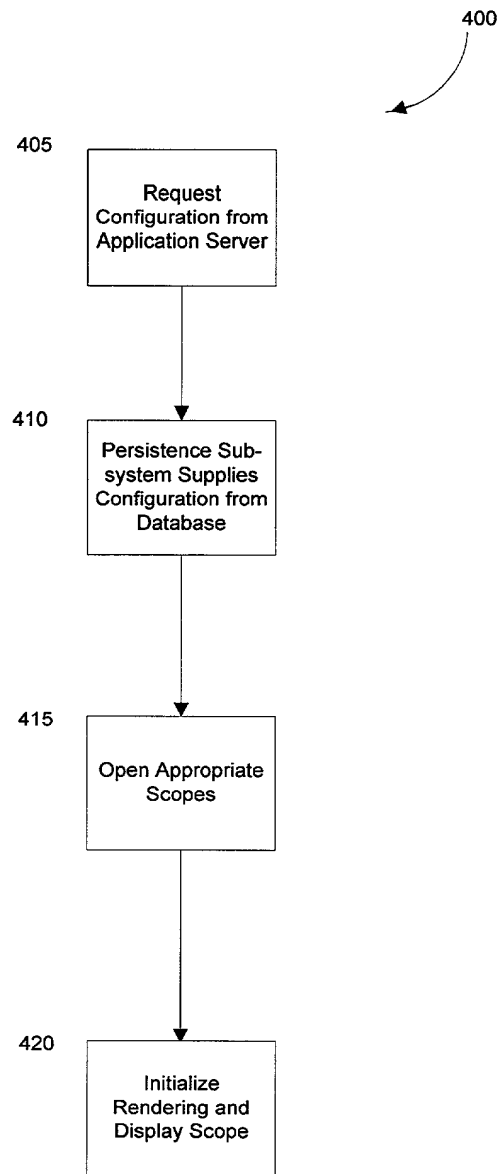


FIG. 4

CREATE A SCOPE

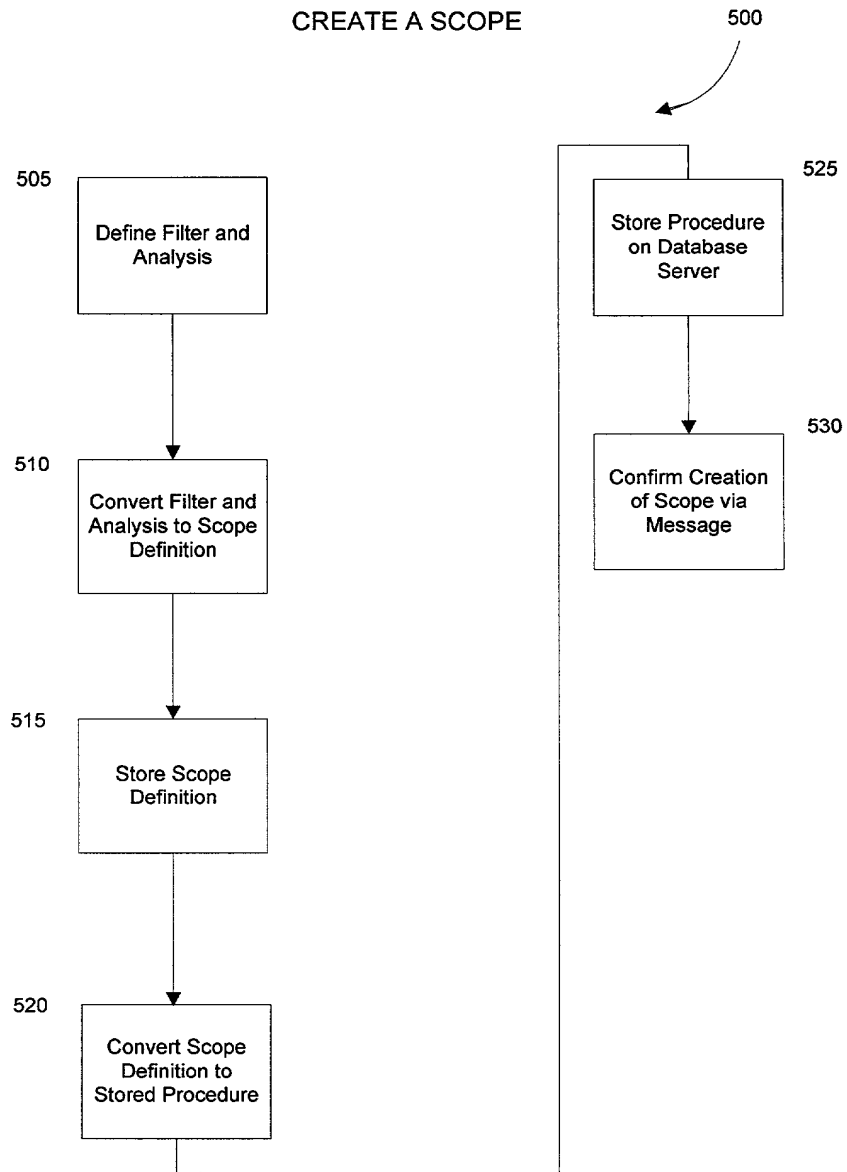


FIG. 5

EDIT A SCOPE

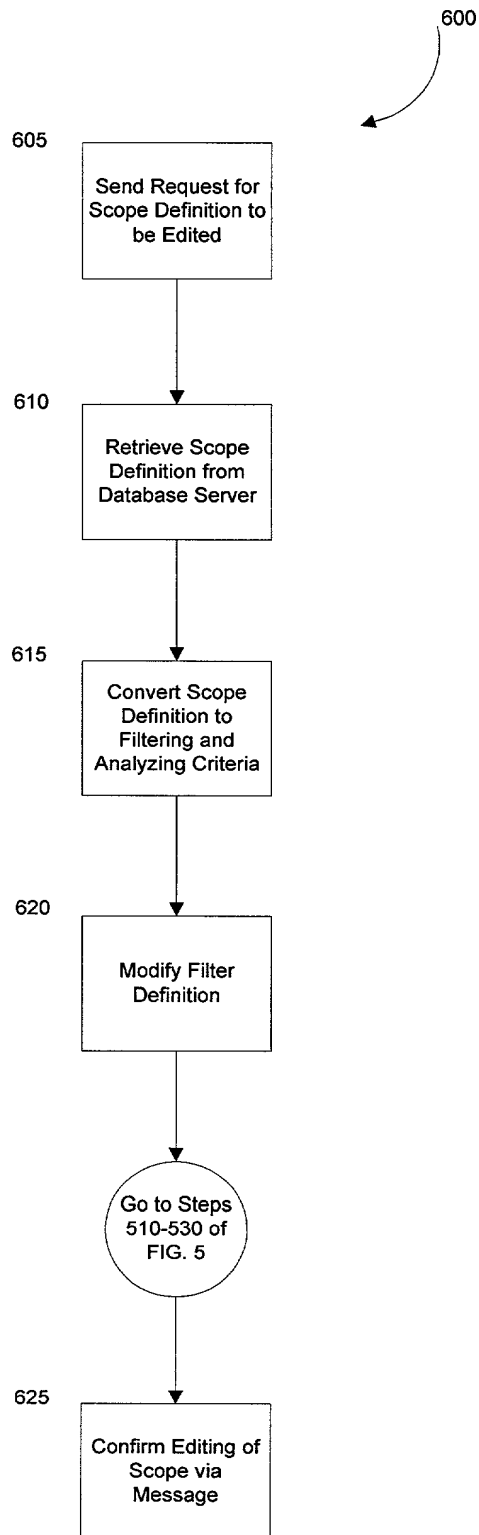


FIG. 6

DELETE A SCOPE

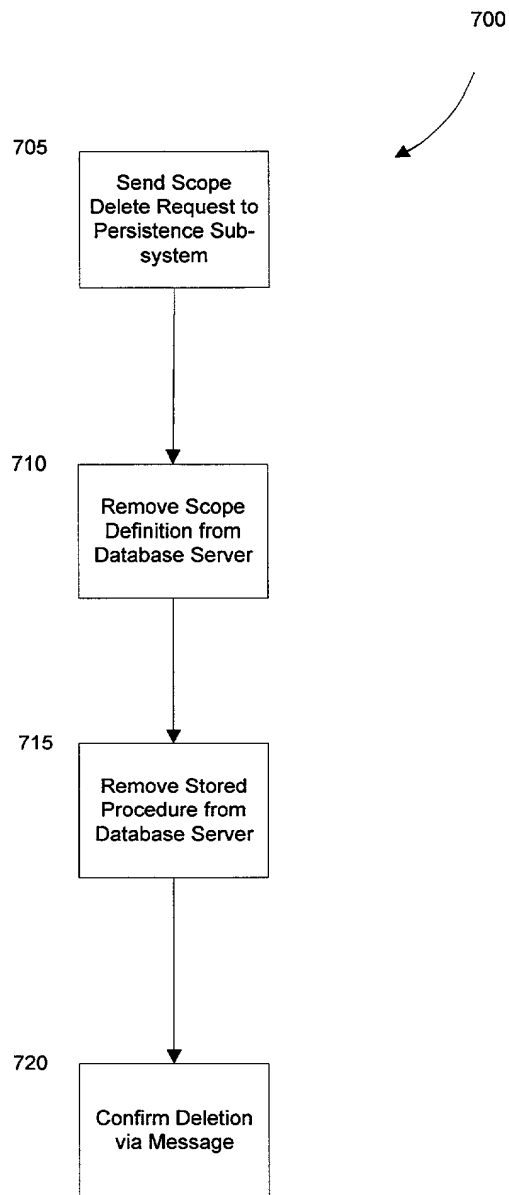


FIG. 7

DATA COLLECTION

800

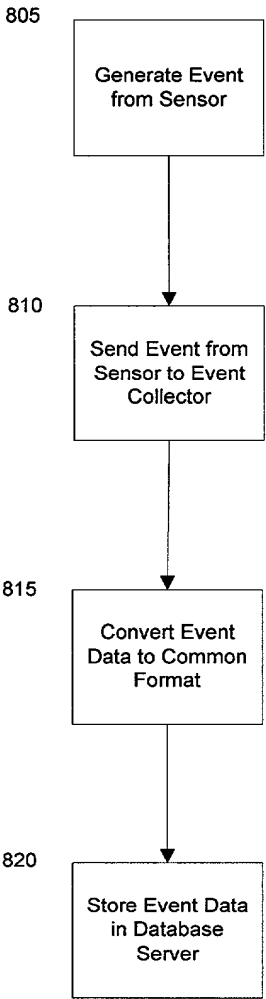


FIG. 8

ANALYSIS

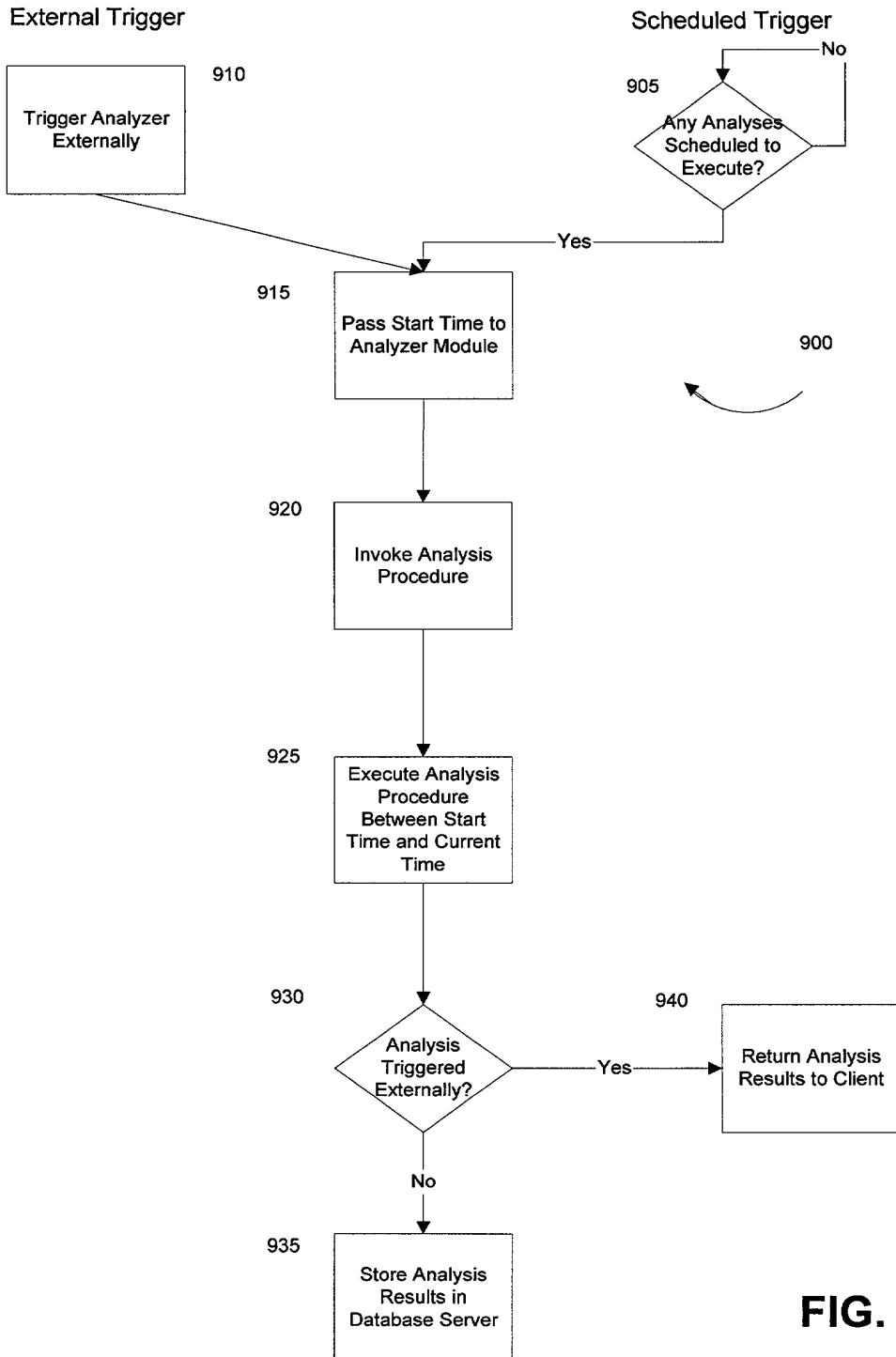


FIG. 9

MONITORING/ POLLING FOR DATA

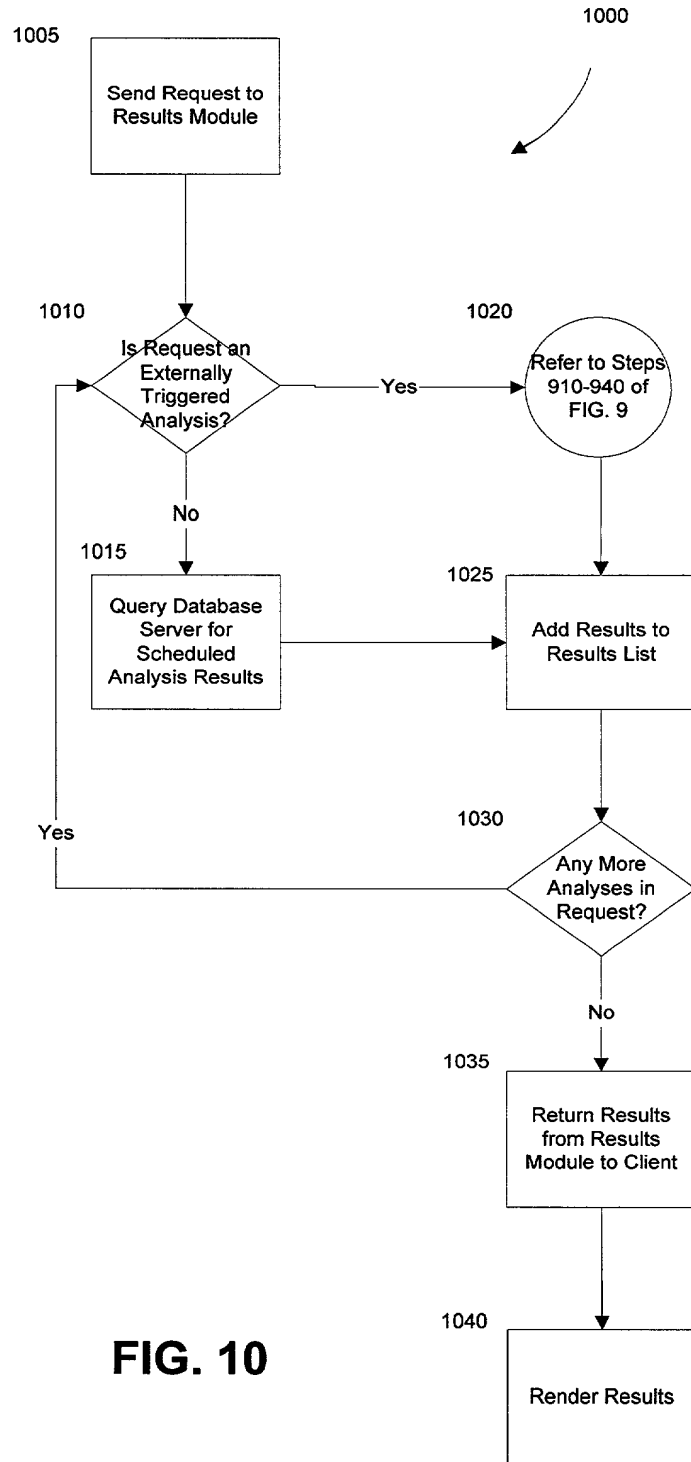


FIG. 10

MONITORING/ POLLING FOR MESSAGES

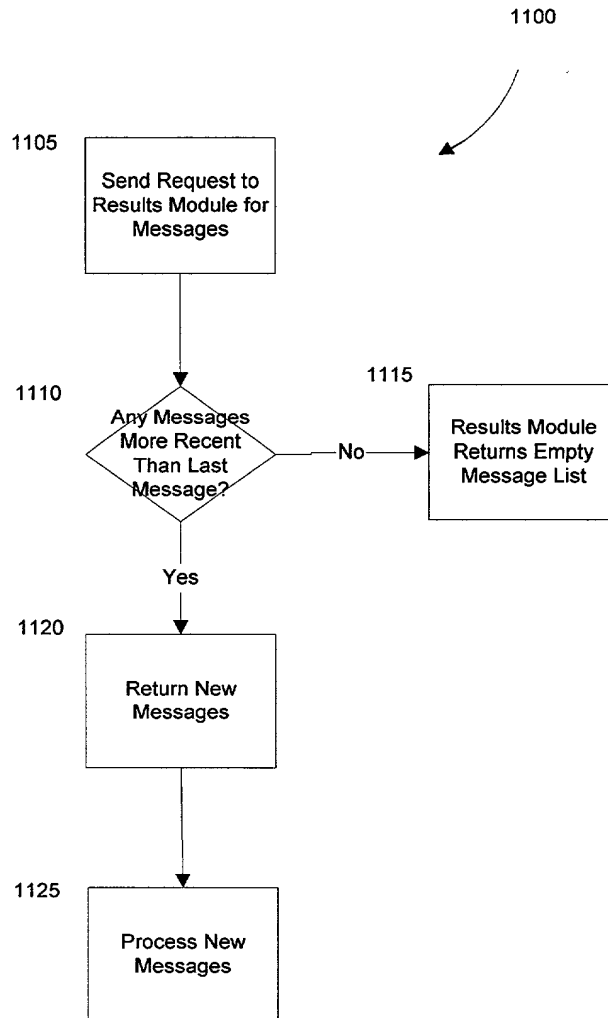


FIG. 11

REQUESTING EVENT DETAILS

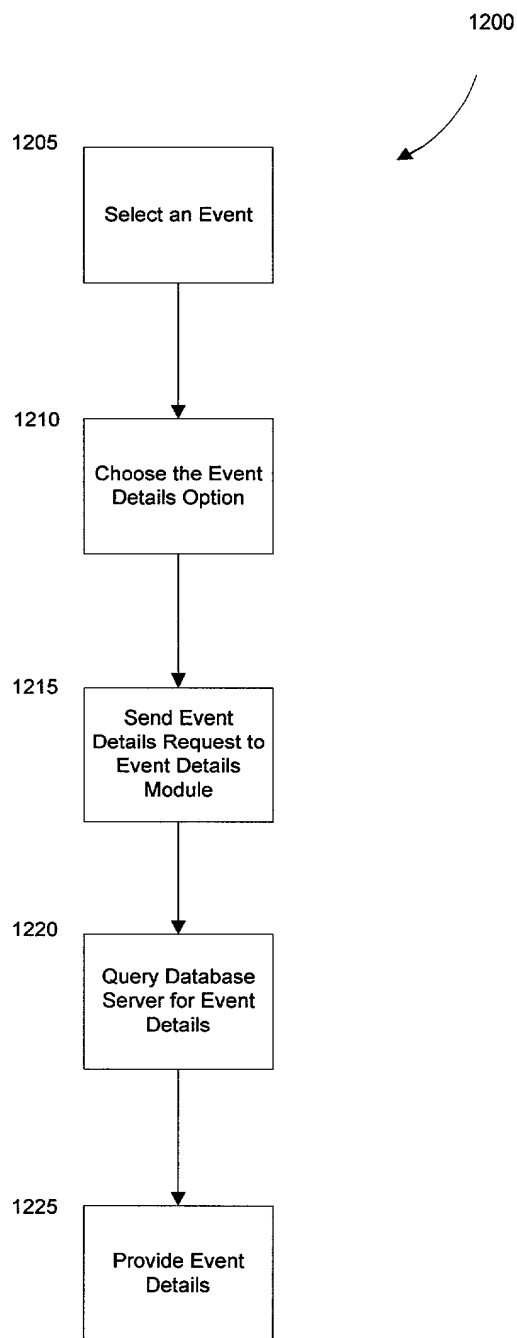


FIG. 12

CLEAR AN EVENT

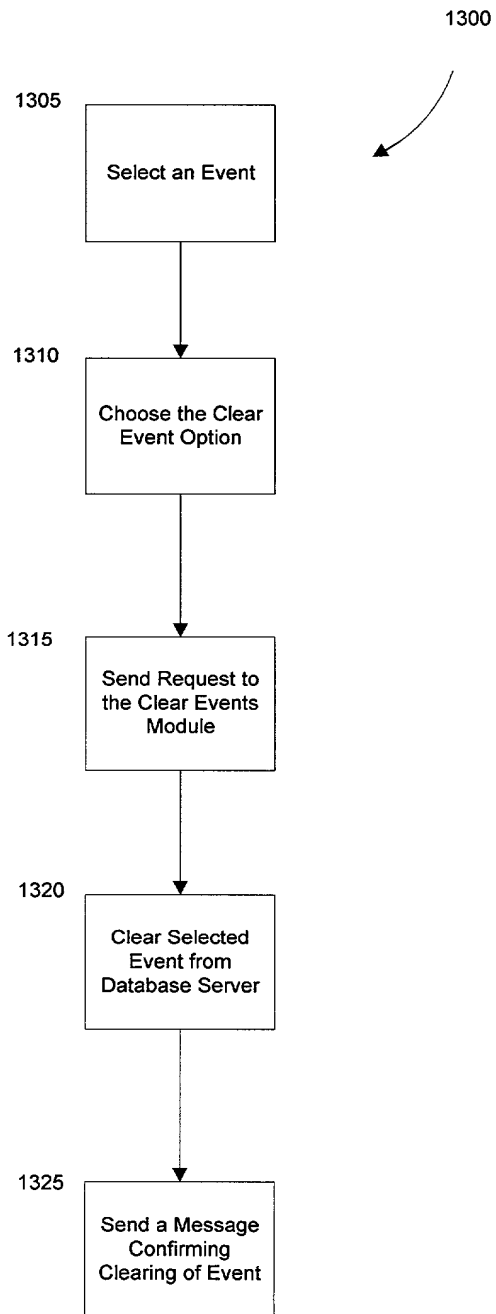


FIG. 13

CREATE INCIDENT

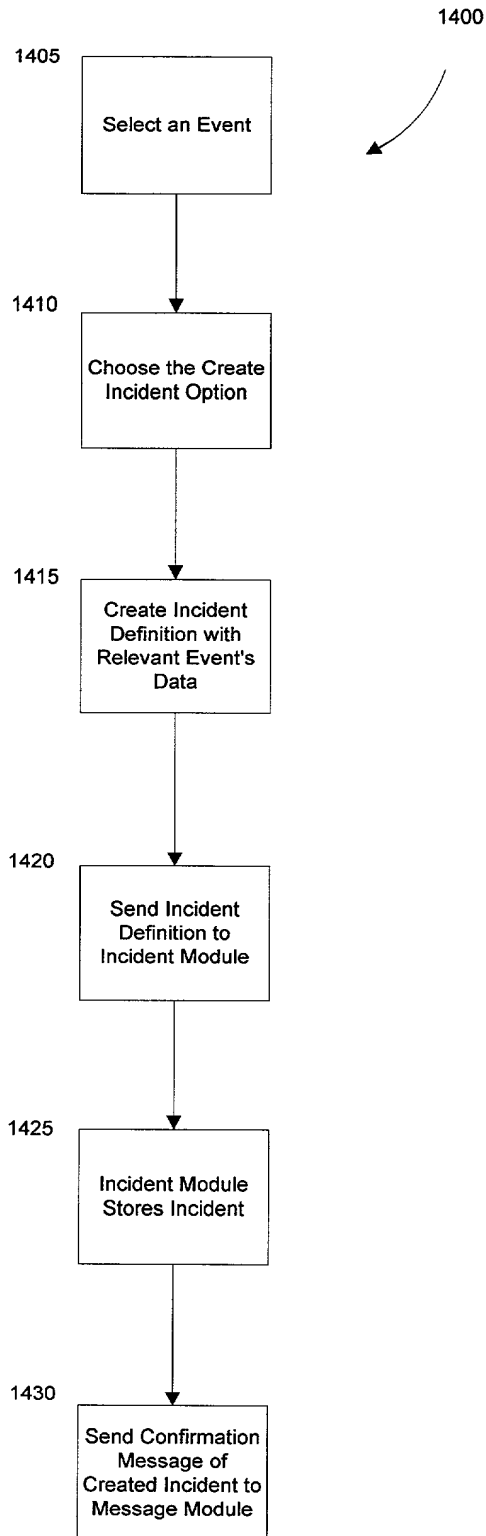


FIG. 14

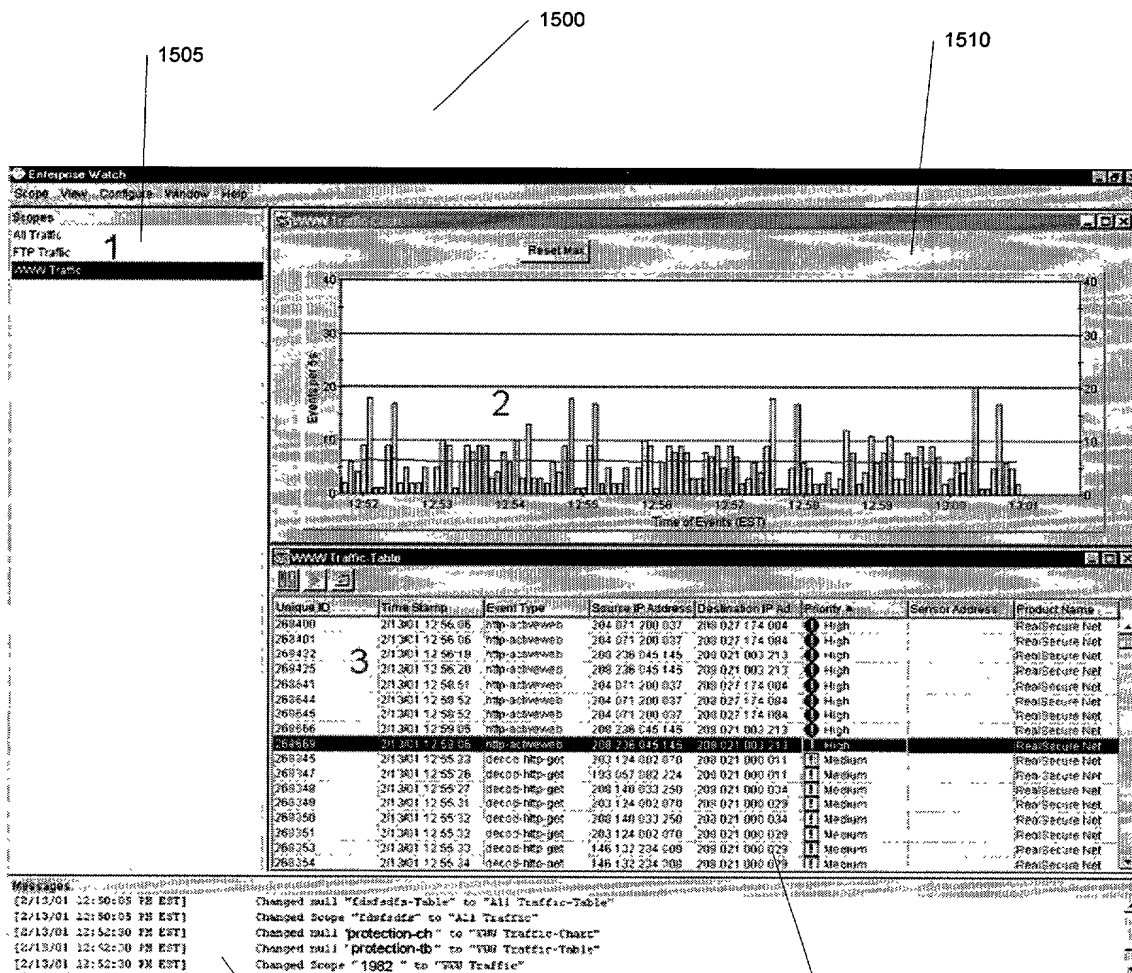


FIG. 15

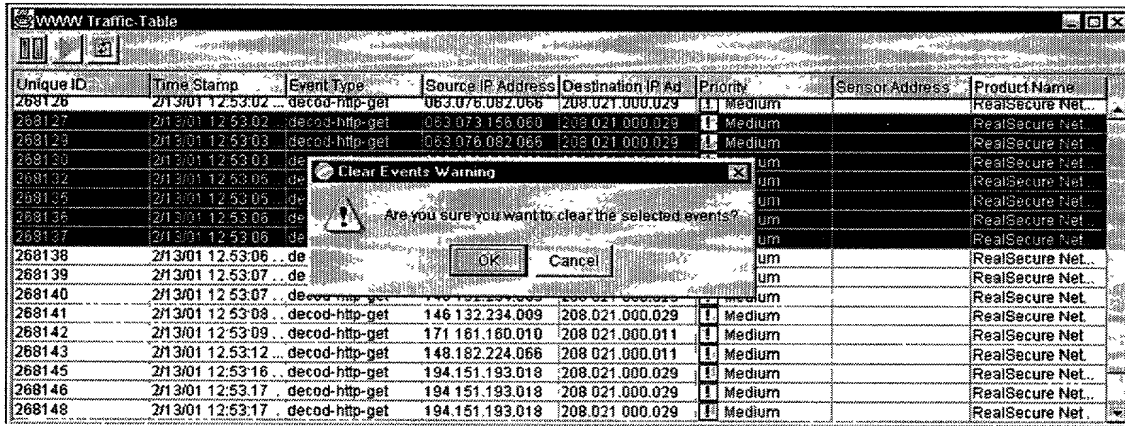
1600

1605

Unique ID	Time Stamp	Event Type	Source IP Ad...	Destination I...	Priority ▲	Sensor Addre...	Product Name
271569	2/13/01 1:31:...	http-activeweb	204.071.200...	208.027.174...	High		RealSecure ...
271572	2/13/01 1:31:...	http-activeweb	204.071.200...	208.027.174...	High		RealSecure ...
271573	2/13/01 1:31:...	http-activeweb	204.071.200...	208.027.174...	High		RealSecure ...
271594	2/13/01 1:32:...	http-activeweb	208.236.045...	208.021.003...	High		RealSecure ...
271597	2/13/01 1:32:...	http-activeweb	208.236.045...	208.021.003...	High		RealSecure ...
271632	2/13/01 1:32:...	decod-http-get	194.154.206...	208.021.000...	Medium		RealSecure ...
271639	2/13/01 1:32:...	decod-http-get	194.154.206...	208.021.000...	Medium		RealSecure ...
271640	2/13/01 1:32:...	decod-http-get	156.099.090...	208.021.000...	Medium		RealSecure ...
271641	2/13/01 1:32:...	decod-dns-all	199.191.129...	208.021.000...	Medium		RealSecure ...
271547	2/13/01 1:31:...	smtp-ehlo	206.141.207...	208.021.000...	Low		RealSecure ...
271560	2/13/01 1:31:...	smtp-ehlo	216.094.034...	208.021.000...	Low		RealSecure ...
271599	2/13/01 1:32:...	smtp-ehlo	205.188.157...	208.021.000...	Low		RealSecure ...

FIG. 16

1700



Unique ID	Time Stamp	Event Type	Source IP Address	Destination IP Ad	Priority	Sensor Address	Product Name
268126	2/13/01 12:53:02	decod-http-get	063.076.082.066	208.021.000.029	1 Medium		RealSecure Net...
268127	2/13/01 12:53:02	decod-http-get	063.073.156.060	208.021.000.029	1 Medium		RealSecure Net...
268129	2/13/01 12:53:03	decod-http-get	063.076.082.066	208.021.000.039	1 Medium		RealSecure Net...
268130	2/13/01 12:53:03	decod-http-get	063.076.082.066	208.021.000.039	1 Medium		RealSecure Net...
268132	2/13/01 12:53:05	decod-http-get	063.076.082.066	208.021.000.039	1 Medium		RealSecure Net...
268135	2/13/01 12:53:05	decod-http-get	063.076.082.066	208.021.000.039	1 Medium		RealSecure Net...
268136	2/13/01 12:53:06	decod-http-get	063.076.082.066	208.021.000.039	1 Medium		RealSecure Net...
268137	2/13/01 12:53:06	decod-http-get	063.076.082.066	208.021.000.039	1 Medium		RealSecure Net...
268138	2/13/01 12:53:06	decod-http-get	063.076.082.066	208.021.000.039	1 Medium		RealSecure Net...
268139	2/13/01 12:53:07	decod-http-get	063.076.082.066	208.021.000.039	1 Medium		RealSecure Net...
268140	2/13/01 12:53:07	decod-http-get	063.076.082.066	208.021.000.039	1 Medium		RealSecure Net...
268141	2/13/01 12:53:08	decod-http-get	146.132.234.009	208.021.000.029	1 Medium		RealSecure Net...
268142	2/13/01 12:53:09	decod-http-get	171.161.160.010	208.021.000.011	1 Medium		RealSecure Net...
268143	2/13/01 12:53:12	decod-http-get	148.182.224.066	208.021.000.011	1 Medium		RealSecure Net...
268145	2/13/01 12:53:16	decod-http-get	194.151.193.018	208.021.000.029	1 Medium		RealSecure Net...
268146	2/13/01 12:53:17	decod-http-get	194.151.193.018	208.021.000.029	1 Medium		RealSecure Net...
268148	2/13/01 12:53:17	decod-http-get	194.151.193.018	208.021.000.029	1 Medium		RealSecure Net...

FIG. 17

Scope Configuration

Name: 1 **FTP Traffic**

Description: Scope for monitoring ftp traffic

Calculation Interval: 30 sec

Scope Criteria

Include events which match the following rows:

Destina...	Source...	Event T...	Priority	Sensor	Sensor
		FTP	Medium High		
2					

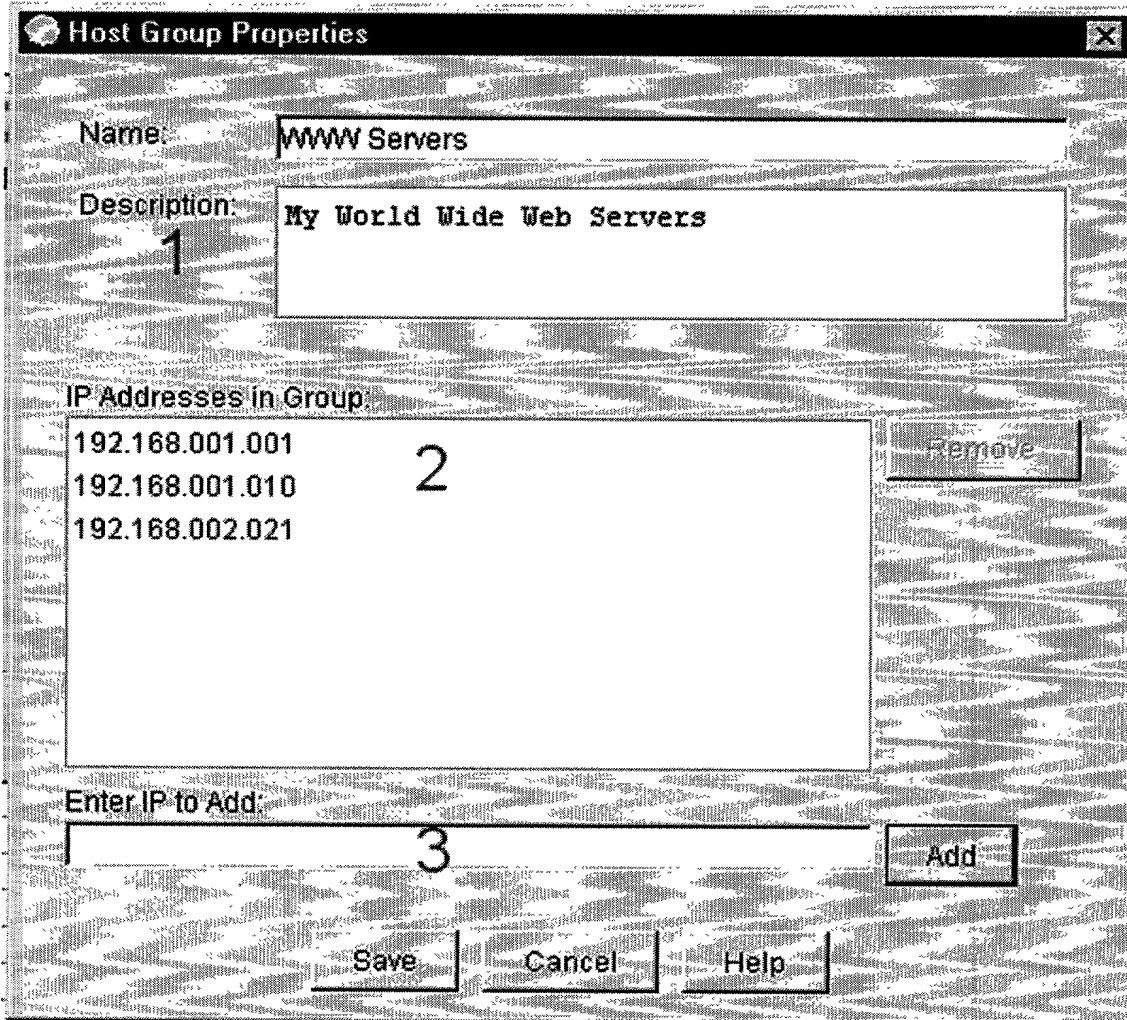
Edit Cell

New Row

Delete Row

Save **Cancel** **Help**

FIG. 18



The image shows a screenshot of a 'Host Group Properties' dialog box. The dialog has a title bar with a close button. It contains several fields and buttons. The 'Name' field is labeled 'Name:' and contains the text 'WWW Servers'. The 'Description' field is labeled 'Description:' and contains the text 'My World Wide Web Servers'. Below the description field is a list box labeled 'IP Addresses in Group' containing three IP addresses: '192.168.001.001', '192.168.001.010', and '192.168.002.021'. To the right of the list box is a 'Remove' button. Below the list box is a text input field labeled 'Enter IP to Add:' with an 'Add' button to its right. At the bottom of the dialog are three buttons: 'Save', 'Cancel', and 'Help'. There are three handwritten numbers: '1' next to the Description field, '2' next to the IP list box, and '3' next to the 'Enter IP to Add:' field.

Host Group Properties

Name: WWW Servers

Description: My World Wide Web Servers

IP Addresses in Group

192.168.001.001

192.168.001.010

192.168.002.021

Remove

Enter IP to Add:

Add

Save Cancel Help

FIG. 19

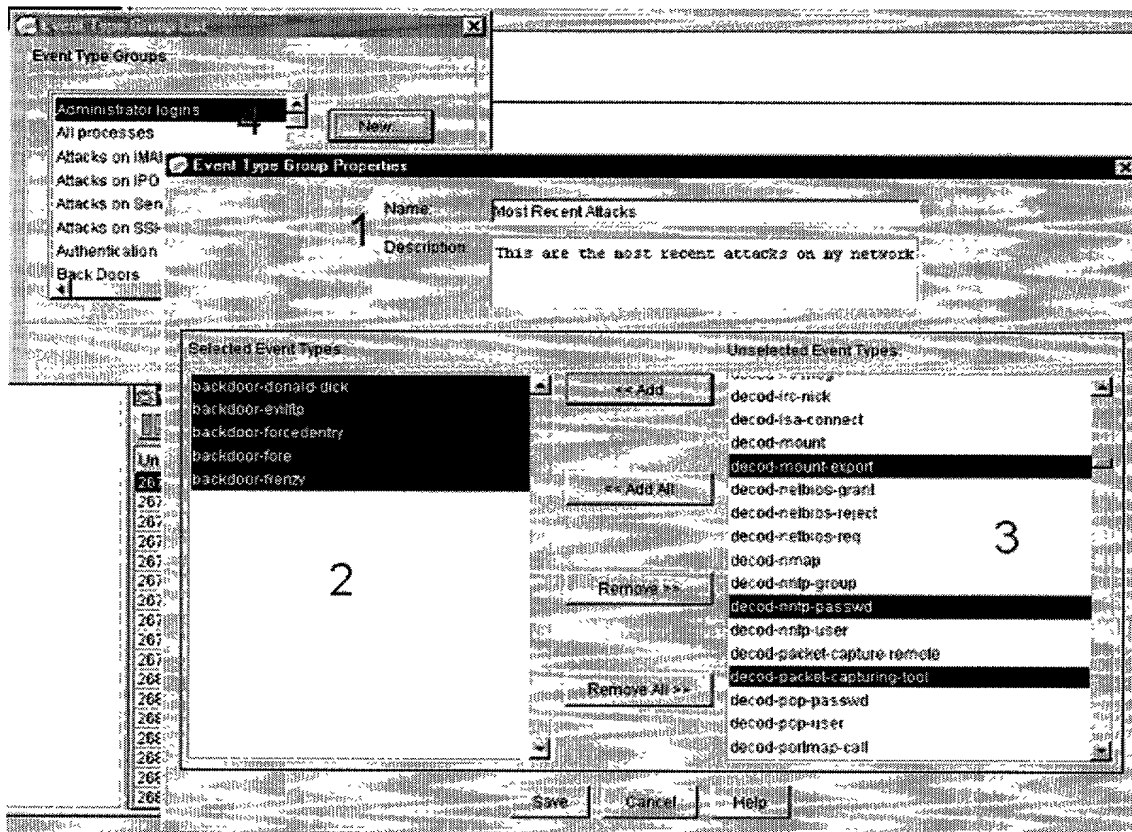


FIG. 20

2100

2105

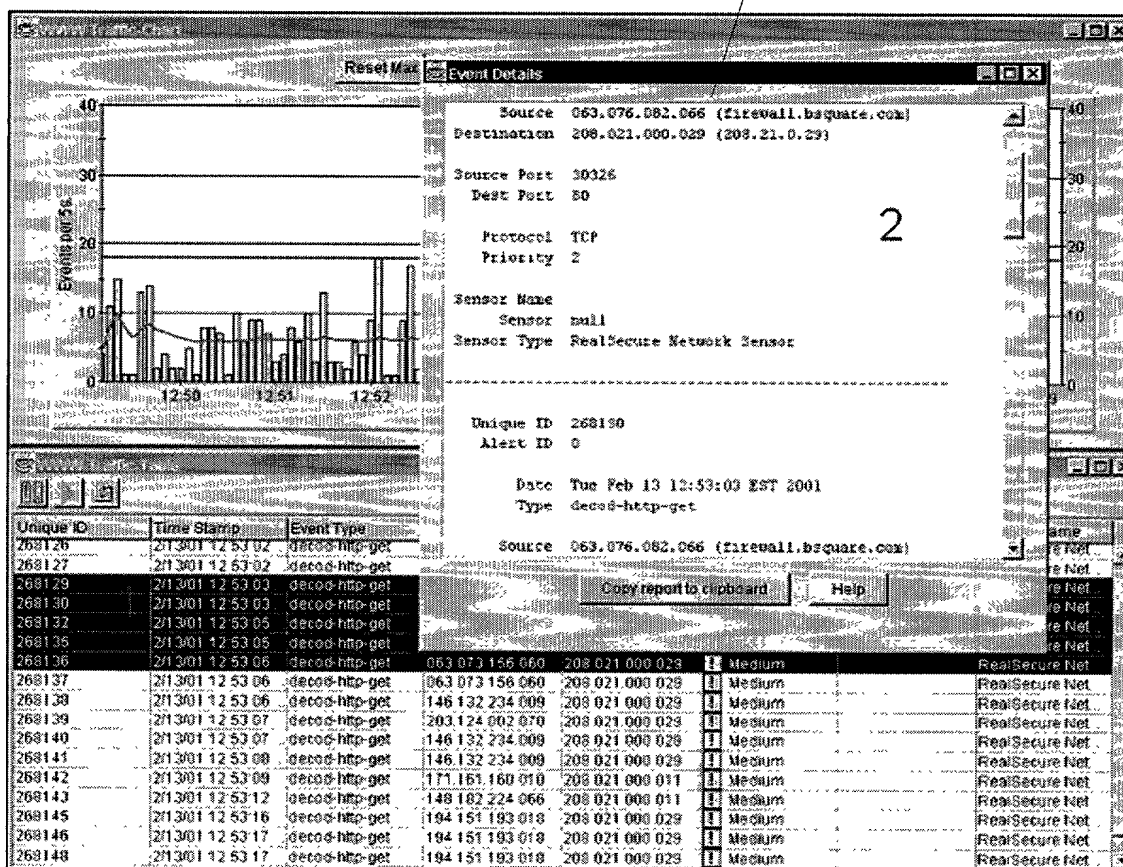


FIG. 21